

09/675,976

Remarks

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. Claims 1, 3, 6, 9, 11, 17, 19, 21, 28, and 29 have been amended. Claims 31-38 have been withdrawn to address Examiner's restriction requirement. Claims 39-40 have been added to recite further embodiments of the invention as previously discussed in Applicants' first response to an Office Action. Claims 1-30 and 39-40 are now pending in the application.

ARGUMENT

Claims 3, 11-13 and 19-30 have been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. This rejection is respectfully traversed and Claims 3, 11-13 and 19-30 are believed allowable based on the above amendments and following discussion.

Claim 3 has been amended to require "said source stream identifier comprising a source of said keys, and *when necessary to provide sufficient information to access said at least one key, a source of said portion of said payload.*" Thus, it should be clear that the source stream identifier comprises a source of said keys, and when the source of said payload is necessary to provide sufficient information to access the key, then the source stream identifier further comprises the source of said portion of said payload.

Claims 11 and 21 have been amended to remove the "if necessary" qualifier. The Examiner erroneously asserts that Claim 19 recites the phrase "if necessary." Applicants note that Claim 21 recites the phrase "if necessary," but that Claim 19 does not. Therefore, Applicants respectfully request that this erroneous rejection be withdrawn. Claim 19 has been amended to change the word "with" to "using" to address the Examiner's objection to the grammar of the claim.

09/675,976

Claims 1-30 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,757,908 to Cooper et al., (hereafter, "Cooper et al."). This rejection is respectfully traversed and Claims 1-30 are believed allowable based on the above amendments and the foregoing and following discussion.

Generally, Cooper et al. teach a system for enabling a file or software application which has been locked from the user. Cooper et al. teach an apparatus for securing access to particular files which are stored in a computer-accessible memory media. A plurality of files is stored in a computer-accessible memory media, including at least one encrypted file and at least one unencrypted file. For each encrypted file, a preselected portion of the file is recorded in memory, a decryption block is generated which includes information which can be utilized to decrypt the file, and the decryption block is incorporated in the file in lieu of the preselected portion which has been recorded in memory.

In contrast, Applicants' invention recites a system for transmitting a data stream made up of data blocks, where a data block portion of a payload may be replaced with a tag indicating whether a decryption key is necessary to decode the data block. The data blocks of a given data stream may contain disparate protocols and be routed to one or more application decoders. Further, the sending device and receiving device may negotiate for a session key to decrypt the decryption keys, thereby enabling additional security to the data stream as it passes through the data safeguarding device. This negotiation is specifically claimed in the provisionally withdrawn claims.

Cooper et al. teach a system where only one portion of a file is encrypted to protect it from being accessed by a user upon a user request to access the file. An operating system level file management program determines whether the user is authorized to access the file and supplies the decryption key. Cooper et al. teach supplying the key by the vendor. Cooper et al. do not teach or suggest that the decryption key is further encrypted by a negotiated session key, nor do they teach a data stream received from a source device, but merely a file drawn from media.

As described in the specification, and recited in the claims, Applicants' invention safeguards data within a device and forwards data of varying protocols to appropriate application decoders. If a data stream contains both audio and video data blocks, the data blocks from the

09/675,976

received data stream may be sent to different application decoders based on their protocol, i.e., audio vs. video formats. Applying the teachings of Cooper et al. to Applicants' invention will result in an operating system level decoder for files and not a safeguarding device that may be implemented in hardware, software, or firmware that receives transmitted data streams without user request.

The Examiner asserts that Cooper et al. disclose all elements of the claims. The independent claims have been amended to more clearly recite that the first system, i.e., the PCX system decrypts a received data block and then re-encrypts at least portions of the data block before sending the encrypted data to the second system, i.e., the application decoder module. While the claims may recite "*encrypting*," this encrypting of the data is a second encrypting, or re-encrypting. The data block is not received in an encrypted mode and then merely passed through to the second system. It is first decrypted. After decrypting by the first device, a portion of the payload may be replaced. At least a portion of the data block is encrypted before transmitting to the second device. Cooper et al. do not teach or suggest this decrypting or re-encrypting. Thus, Claims 1-30 are allowable as amended.

Cooper et al. do not teach a method to re-encrypt a decrypted data stream, but only a method to decrypt a pre-encrypted file on a media device. In contrast, Applicants' claimed invention receives a data stream and encrypts the payload portion of the data blocks in the data stream before sending them to one or more application decoders. The PCX and application decoders may be separate devices, circuits or modules, or they may be part of the same device. Regardless, the PCX and application decoders are part of an overall data safeguarding system. Cooper et al. teach that the encryption occurs on a vendor system and decryption occurs on a user system.

The Examiner asserts that with regard to Claims 2, 10 and 20, that the encrypting step includes encrypting of the entire payload. Claims 39-40 have been added to more clearly recite that a portion of the payload is encrypted. Cooper et al. do not teach the act of encrypting a portion of the payload in Col. 3, lines 57-59. Cooper et al. teach that a pre-encrypted file is placed in memory and a decryption block is generated to facilitate decryption. Thus, applying Cooper et al. to Applicants' invention would not yield a data safeguarding system which maintains encrypted data to be transmitted within the device. Applying the teachings of Cooper

09/675,976

et al. would allow Applicant to decrypt a file and data safeguarding would end once the file had been decrypted.

Regarding Claims 5 and 28, the Examiner asserts that Cooper et al. teach receiving a stream of data from a third system. (Col. 3, lines 9-15) Cooper et al. do not teach receiving a data stream, whether from a third system or elsewhere. Cooper et al. (Col. 3, lines 9-15) teach receiving a *software object* from a source. Cooper's software object is not analogous to a data stream comprising data blocks which may be sent and decrypted separately. The Examiner asserts that a definition of a data stream is "[a]n undifferentiated, byte-to-byte flow of data." This definition is not synonymous to a software object. A software object is static. It may comprise one or more data blocks. However, the software object is not a "stream of data." It does not flow, as in Examiner's provided definition. For instance, a stream of data may comprise disparate blocks of unrelated information. A software object demands that the data blocks are related blocks of information. Thus, Applicants maintain the assertion that Cooper et al. does not teach or suggest a "stream of data" received by the first system. Applicant further discloses that separate data blocks within the same data stream may be sent to one or more (at least one) application decoders (Claim 28, as amended), thus, not maintaining the data stream as one entity, as taught by Cooper et al.

Applicants provisionally withdraw Claims 31-38. However, the restriction requirement asserted by the Examiner is respectfully traversed. Claims 31-38 recite elements of the disclosed invention that have been previously argued in Applicants' first office action response. It is not believed that the scope of these claims rise to the level of requiring a new search. However, in an effort to expedite the Examination of Claims 1-30 and 39-40, Applicants withdraw consideration of Claims 31-38.

Thus, for the foregoing reasons, all claims remaining in the application are now allowable.

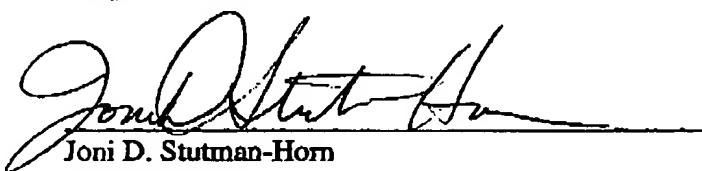
09/675,976

CONCLUSION

In view of the foregoing, Claims 1-30 and 39-40 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 4/6/2005



Joni D. Stutman-Horn
Patent Attorney
Intel Corporation
Registration No. 42,173
(703) 633-6845

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026